2016

The Fourth Amendment in the Digital World: Do You Have an Expectation of Privacy on the Internet?

Brian M. Kistner

The Fourth Amendment of our Constitution provides a safeguard for U.S. citizens against government intrusion by barring "unreasonable searches and seizures."[1] The Supreme Court, however, has faced significant difficulty in consistently determining what government actions are "unreasonable" and what actions constitute a "search" or "seizure." The Court's enduring problems have led several legal scholars to criticize the Supreme Court's Fourth Amendment jurisprudence as "famously zigzagging,"[2] and creating a legal framework that is riddled with inconsistency and incoherence.[3] As a result, many in the legal community have acknowledged that Fourth Amendment doctrine is in a state of theoretical chaos.[4] This is especially true regarding the Court's approach to Internet surveillance. An analysis of the Fourth Amendment doctrine over the years leads to the inevitable conclusion that case law and federal legislation are currently ill-equipped to address Internet privacy rights.

In the eighteenth and early nineteenth centuries, the Fourth Amendment played a minor role in search and seizure cases.[5] One of the Court's earliest decisions held that the "contents" of letters and sealed packages were "fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their domiciles."[6] What limited role it did play early on, the Supreme Court's early Fourth Amendment doctrine strictly construed the amendment to protect *only* against the government's

[1] U.S. Constitution ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").
[2] David A. Sklansky, *Back to the Future: Kyllo, Katz, and Common Law*, 72 Miss. L.J. 143, 143 (2002).
[3] Daniel J. Solove, *Fourth* Amendment Pragmatism, 51 B.C. L. Rev. 1511, 1511 (2010).
[4] Id at 1512.
[5] Colin Shaff, *Is the Court Allergic to Katz? Problems Posed by New Methods of Electronic Surveillance to the "Reasonable-Expectation-of-Privacy" Test*, 23 S. Cal. Interdisc. L.J. 409, 414 (2014)
[6] *Ex parte Jackson*, 96 U.S. 727, 728 (1877).

physical trespasses onto a citizen's property, the warrantless search of tangible personal property, or the warrantless seizure of the person.[7] The National Prohibition Act of 1919, however, led to an exponential increase in the number of federal prosecutions.[8] Consequently, the resulting use of telephone wiretaps by federal investigators led to constitutional challenges to federal searches.

United States v Olmstead epitomizes the Supreme Court's early Fourth Amendment jurisprudence. [9] In *Olmstead,* the defendant Roy Olmstead sought to suppress, as a constitutionally impermissible search, recordings of conversations obtained by the police after a lengthy months-long wiretap of his home and office telephone lines.[10] The Court held that the Fourth Amendment's guarantee of a right to be secure in one's "persons, houses, papers, and effects" only provided protection against searches and seizures of "tangible things."[11] Under this rationale, the Court found that a wiretap was not a Fourth Amendment search so long as the government did not "physically penetrate the houses or offices of the defendants" in placing the wiretap.[12] Consequently, the majority concluded that the wiretap was not a search under the Fourth Amendment for two primary reasons: 1) there was no physical invasion of a constitutionally protected area as there was no physical trespass onto Olmstead's real property and 2) there was no search of a tangible item as the wiretap searched only intangible sound.[13]

In his dissent, Justice Brandeis cautioned the Court in *Olmstead* that it was their duty to develop and adapt the Fourth Amendment in such a way as to guard against, not only means of

[7] *Olmstead v. United States*, 277 U.S. 438, 465 (1928)
[8] Id. at 466
[9] Amanda Yellon, *The Fourth Amendment's New Frontier: Judicial Reasoning Applying the Fourth Amendment to Electronic Communications*, 4 J. Bus. & Tech. L. 411, 415 (2009)
[10] *Olmstead*, 277 U.S. at 455
[11] Id. At 464
[12] Id. at 466
[13] Id.at 464

government intrusion then known, but also "what may be" in the future.[14] Brandeis further predicted that the technology of government intrusion into the private lives of its citizens would not stop with the advent of wiretapping,[15] but would extend to "the most intimate occurrences of the home" without even "removing papers from secret drawers.[16]

Justice's Brandeis' "right to be let alone" philosophy in *Olmstead* did not immediately catch on.[17] Over the next four decades, the Court continued to adhere to its physical intrusion requirement enunciated in *Olmstead.* For instance, in *Goldman vs United States*, the Court held that the government did not trigger Fourth Amendment coverage by placing a listening device against an outer wall of a building and listening to private conversations within.[18] The Court continued to rely on *Olmstead* in *Silverman v United States* and *Clinton v Virginia*. In both of those holdings, the Court reasoned that physical intrusion by the government was required for a petitioner to seek Fourth Amendment protection.[19] It was becoming clear, however, that the Court's physical trespass-based test was being manipulated by the government's new and innovative wiretapping techniques. In *Clinton v Virginia*, for example, the government attached a listening device using means that merely causing a thumbtack sized penetration in a wall. *Olmstead's* rule barely survived in that case, but the Court did conclude that the minuscule physical intrusion constituted a "search" within a meaning of the Fourth Amendment.[20]

---

[14] Id. at 474 (Brandeis, J., dissenting).
[15] Yellon, 4 J. Bus. & Tech. L at 415
[16] Olmstead, 277 U.S. at 474 (Brandeis, J., dissenting).
[17] "The makers of our Constitution ... conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men." *Olmstead,* 277 U.S. at 478 (Brandeis, J., dissenting).
[18] *Goldman v. United States*, 316 U.S. 129, 135 (1942)
[19] *Silverman v. United States*, 365 U.S. 505, 511 (1961)
[20] *Clinton v. Virginia*, 377 U.S. 158 (1964)

With it becoming easier for the Government to listen in on conversations without physically trespassing onto a person's property, the Court and the legal community were becoming concerned that nothing would soon be left of Fourth Amendment protection. A new privacy test was needed. In response to that need, the Court brought vitality back to the Fourth Amendment in the revolutionary case of *Katz v United States*.

In *Katz*, the government was permitted at trial, over Katz's objection, to introduce evidence of Katz's telephone calls overheard by FBI agents. Specifically, the FBI had attached a bug to the outside of a public phone booth from which Katz made his calls. The Court of Appeals, relying on the *Olmstead* trespass-based rule, affirmed the lower court ruling. On appeal, however, the Supreme Court reversed and found that the FBI's bugging of the outside of a phone booth constituted an unlawful search, thereby violating Katz's Fourth Amendment rights. The Court held that, through their warrantless search, the FBI violated "the privacy upon which defendant [Katz] justifiably relied."[21] Justice Stewart, in delivering the majority opinion, stated that the Fourth Amendment "protects people, not places."[22] The Court opined that what a person seeks to preserve as private, regardless of his location, may be constitutionally protected under the Fourth Amendment. By expanding the scope of the amendment, the Court departed from the limiting and narrow view of *Olmstead*.[23]

Justice Harlan, in his concurrence in *Olmstead*, elaborated on the Court's new Fourth Amendment privacy standard. He explained that the phone booth in *Katz* was "an area where,

[21] *Katz v United States*, 389 U.S. 347 (1967).
[22] *Id.* at 350.
[23] "Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure." *Id.* at 353 (Stewart for majority)

like a home, a person has a constitutionally protected reasonable expectation of privacy."[24] Harlan commented that, in addition to a physical intrusion by the government, an "electronic" intrusion could also constitute a violation of the Fourth Amendment.[25] In establishing an expectation of privacy threshold test, Harlan explained that for a person like Katz to seek Fourth Amendment protection, he has the burden of satisfying a "twofold requirement."[26] Specifically, for a person to show that the government violated his/her Fourth Amendment rights, that person must, one, exhibit an subjective expectation of privacy (e.g. he seeks to preserve something as private), and two, that person's subjective expectation, viewed objectively, is justifiable under the circumstances.[27] Therefore, if both prongs of Harlan's test are satisfied, then under *Katz*, a person has Fourth Amendment protection and any invasion of that constitutionally protected area is presumptively unreasonable in the absence of a search warrant.[28]

Through its holding in *Katz*, the Court attempted to bring Fourth Amendment law into the world of new technologies by introducing the reasonable expectation of privacy test.[29] The decision provided a long awaited opportunity for the Court to broaden Fourth Amendment protection. Many descendant cases followed whose task was to develop, refine, and delimit the boundaries of the privacy doctrine of *Katz.* One such case was *Smith v Maryland*[30], through which Justice Harlan's expectation of privacy test was applied and, in turn, explained more precisely.

[24] *Id.* at 360.
[25] *Id.*
[26] *Id.* at 361.
[27] *Id.*
[28] *Id.*
[29] Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 585 (2005)
[30] *Smith v Maryland*, 442 U.S. 735 (1979).

In *Smith v Maryland,* a harassment case, a woman reported to the police that not only was she robbed by Smith, but was also receiving threatening phone calls from him thereafter. As part of their investigation, the police installed a device ("pen register") at a telephone company's central office to intercept the phone numbers dialed by Smith in an effort to determine if he was in fact calling the complainant. As a result of utilizing the pen register, the police did find that Smith made phone calls to the complainant and subsequently arrested him. Smith was later convicted. After multiple appeals, the Supreme Court set out to determine whether the government, like in *Katz*, infringed on Smith's reasonable expectation of privacy. Using Harlan's twofold test, the Court held that the use of the pen register did not constitute a "search" under the Fourth Amendment.[31]

The *Smith* Court concluded that, given the limited capabilities of the pen register (i.e. only discloses phone numbers dialed and not conversations), Smith's claim that he had a legitimate expectation of privacy must be rejected.[32] Implementing Harlan's test, the Court found that people do not subjectively have any subjective expectation of privacy in the phone numbers that they dial. Moreover, the Court deemed that society would also not objectively find that an expectation of privacy in dialing phone numbers to be a reasonable one.[33]

Likening the pen register as a modern day equivalent to the early day switchboard operator, the *Smith* Court relied on the concept of third-party doctrine in justifying their holding. As Justice Blackmun commented, the Court has "consistently held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third-parties."[34] Applying that principle in *Smith*, the Court determined that when people, like Smith, whom

[31] *Id.* at 746.
[32] *Id.* at 742.
[33] *Id.*
[34] *Id.* at 744.

voluntarily convey information to third parties, like a communications company, they expose that information to the company's equipment. As a result, people like Smith must assume the risk that the communications company could reveal that information to law enforcement.[35]

Opposing the majority's view in *Smith*, Justice Stewart believed that the use of the pen register constituted a warrantless search. Relying on *Katz*, his dissent hinged on the presumption the numbers dialed from a private telephone are the same as the conversations that occur during a phone call, and therefore are within Fourth Amendment protection.[36] Justice Stewart opined that the phone numbers, while mundane in comparison to an actual telephone conversation, still contain "content" that requires constitutional safeguards.[37] In explaining his position, Stewart doubted that people would be alright with the list of the phone numbers they dialed being "broadcast to the world" because such a list could reveal the "identities of the persons and the places called, and thus reveal the most intimate details of a person's life."[38]

Justice Marshall also dissented in *Smith* and, like Justice Stewart, applied Harlan's privacy test in concluding that a legitimate expectation of privacy did exist in the dialing of phone numbers. Marshall commented that the majority erred in applying *Katz* and the third party doctrine to the facts of the case.[39] Focusing on third party doctrine, Marshall opined that a person is incapable of assuming the risk of disclosure by third parties to the government when no realistic alternatives exist. Specifically, Marshall commented that "implicit in the concept of assumption of risk is the notion of choice."[40] Without having the option of choice, therefore,

---

[35] *Id.*
[36] *Id.* at 747.
[37] *Id.* at 748.
[38] *Id.*
[39] "The crux of the Court's holding, however, is that whatever expectation of privacy petitioner may in fact have entertained regarding his calls, it is not one "society is prepared to recognize as 'reasonable'." In so ruling, the Court determines that individuals who convey information to third parties have "assumed the risk" of disclosure to the government. This analysis is misconceived…" *Id.* at 478 (Marshall, T., dissenting).
[40] *Id.* at 749.

there can be no risk. So, applied to the facts in *Smith,* unless the defendant unrealistically chose not to use the phone altogether, he had no choice but to accept the risk of government surveillance.[41]

Justice Marshall called upon the Court to base the *Katz* expectation of privacy analysis, not on one's assumption of risk of disclosing to third parties but rather, on the risks one should be forced to assume in a free society.[42] Based on that perspective, and considering the crucial role telephonic calls plays in our day to day lives, Marshall concluded that the expectation of privacy test was satisfied and the government could not obtain the list of phone numbers absent a warrant based on probable cause.[43] Despite its conflicting views, the Court in *Smith* seemed to be making headway in applying *Katz's* expectation of privacy test to advancing methods of electronic surveillance.

In 2001, the Court again addressed the interplay of advancing technology and privacy in *Kyllo v United States.*[44] In *Kyllo*, the government suspected a person, through the use of high intensity heat lamps, was growing marijuana in his home.[45] To confirm its suspicion, the government positioned itself across the street from the suspect's home and, by using a thermal imaging device, determined that the suspect's garage was "relatively hot" compared to the rest of the house.[46] Based on the thermal imaging results, the government obtained a search warrant and found 100 plants growing inside the suspect's home.[47] The case was ultimately brought up to the Supreme Court to address the intrusiveness of the thermal imaging device and whether the government's use of that technology constituted a search under the Fourth Amendment.

---

[41] *Id.*
[42] *Id.* at 750.
[43] *Id.* at 751.
[44] *Kyllo v United States*, 533 U.S. 27 (2001).
[45] Id. at 27.
[46] Id.
[47] Id. at 30.

Kyllo presented the Court with an opportunity to determine the limits on the "power of technology to shrink the realm of guaranteed privacy.[48] Justice Scalia began the majority opinion by underscoring a key point, stating, "It would be foolish to contend that the degree of privacy secured by the Fourth Amendment has been entirely unaffected by the advance of technology."[49] Reiterating Harlan's expectation of privacy standard from *Katz*, the Court found that government's use of the thermal imaging technology violated the suspect's Fourth Amendment rights. In response to concerns about future technological development, the Court established a "bright-line" rule regarding government surveillance that was "not in public use." Scalia elaborated on this rule stating, "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area…constitutes a search - at least where the technology in question is not in general public use."

The majority opinion in *Kyllo* highlighted the Court's concern about technological development and its reluctance to open the door to certain types of warrantless searches. In the end, the decision constituted a successful adaptation of the *Katz* approach to the digital world. As Scalia commented, "reversing that approach (Katz) would leave the homeowner at the mercy of advancing technology."[50] In *Kyllo,* the Court made a clear step forward in Fourth Amendment law. It relied on the expectation of privacy rules of *Katz* and adapted those rules to "more sophisticated systems" of surveillance.[51] However, about ten years later, the Court would take a

[48] Id. at 34.
[49] Id. at 34.
[50] Id at 28.
[51] Id. at 36.

step in a direct direction in Fourth Amendment doctrine. In *Jones v United States,*[52] the Court shied away from the *Katz* standard and proceeded down a different privacy road.

In *Jones,* the Court unanimously concluded that law enforcement installing a GPS tracking device on the underside of a criminal suspect's car did qualify as a "search" under the Fourth Amendment. However, the Court was sharply divided as to why it was a search. Many in the legal community assumed that the Court would continue to apply the *Katz* expectation of privacy test to determine if the four-week long GPS tracking by police constituted a search. Switching course in its Fourth Amendment analysis, the Court surprisingly reverted back to the archaic trespass doctrine from *Olmstead*. According to the majority, by installing the GPS device, there was a physical intrusion of private property for the purposes of obtaining information.[53] Due to the physical intrusion, the Court chose to bypass the *Katz* standard and utilize the narrow, and all but abandoned, physical trespass standard. Justice Scalia explained that the trespass test was the more appropriate test for the facts in *Jones*, and moreover, that Jones' rights should not solely depend on whether he reasonably believed his privacy was violated.[54]

A key question resulting from the *Jones* decision was why Justice Scalia used the *Olmstead* trespass test over the *Katz* expectation of privacy test. In explaining why the Court switched back to the *Olmstead* test, Justice Scalia commented that the "Katz reasonable-

[52] *United States v Jones,* 132 S. Ct. 945 (2012)
[53] *Id*. at 946.
[54] The Government contends that the Harlan standard shows that no search occurred here, since Jones had no "reasonable expectation of privacy" in the area of the Jeep accessed by Government agents (its underbody) and in the locations of the Jeep on the public roads, which were visible to all. But we need not address the Government's contentions, because Jones's Fourth Amendment rights do not rise or fall with the Katz formulation. At bottom, we must "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Id*. at 950.

expectation-of-privacy test has been added to, but not substituted for, the common-law trespassory test."[55] However, that comment, squarely conflicted with Justice Stewart's comments in *Katz.*[56] So, the question remains as to why Justice Scalia based the Court's decision on a supposedly abandoned privacy test. One can only speculate, but perhaps with the country's pervasive use and reliance on technology to communicate, Scalia may have felt society's expectation of privacy was eroding. Perhaps, with social media taking over the way people interact, Scalia was concerned what privacy rights people now considered to be "reasonable." Along these lines, Scalia may have feared that the *Katz* test could no longer offer Fourth Amendment protection. As a result, Scalia may have felt that the trespass doctrine of *Olmstead* was needed to come back into the fray to help bolster the amendment. Whatever Scalia's motivation, it is abundantly clear today that technology is going to eclipse the narrow holding in *Jones* as law enforcement can use methods such as OnStar or cell phone based GPS to track people, without needing to make any physical contact with a car.[57] Additionally, the government can surveil people in other ways, including by monitoring Web traffic or phone or credit card records.

The concurrence in *Jones* disagreed with Scalia's rationale and opined that the Court's reliance on the trespass doctrine was unwise. Justice Alito, for example, concurred in the majority's judgment but based his analysis on the *Katz* privacy test. Accordingly, Alito categorized the issue in *Jones* not as an invasion of property, as Justice Scalia had, but as an invasion of privacy.[58]

---

[55] *Id*. at 947.
[56] "Thus, although a closely divided Court supposed in Olmstead that surveillance without any trespass and without the seizure of any material object fell outside the ambit of the Constitution, we have since departed from the narrow view on which that decision rested." *Katz,* 389 U.S. at 353.
[57] The Honorable M. Margaret McKeown, *The Internet and the Constitution: A Selective Retrospective*, 9 Wash. J.L. Tech. & Arts 135, 166 (2014).
[58] *Id.*

Justice Sotomayor's enlightening concurrence in *Jones* expressed a more expansive approach to privacy issues.[59] Sotomayor suggested that the government's ability to obtain "at a relatively low cost such a substantial quantum of intimate information about any person" required adapting and expanding the *Katz* expectation of privacy test.[60] Sotomayor also questioned, and took on the continuing viability of, the third party doctrine; a theory many believe creates the largest gap in privacy protection, especially in the realm of technology.[61] Specifically, Sotomayor commented, "It may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties…This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers…"[62] Condemning third party doctrine as applied to these technologies, she commented, "I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year."[63] Unlike permissible third party search cases of the past, Sotomayor sought to emphasize the Court's attention of the copious and unparalleled amounts of information individuals disclose to telecommunication companies and Internet service providers in the digital age.

In contrast to every other Justice in *Jones*, Sotomayor reasoned that evolving digital technology had essentially changed the meaning of what "privacy" when myriads of personal

[59] Shaff, *supra* at 432.
[60] *Jones*, 132 S. Ct. at 955-56 (Sotomayor concurring). See also Shaff, *supra* at 432-433.
[61] Richard M. Thompson II, *United States v. Jones: GPS Monitoring, Property, and Privacy*, https://www.fas.org/sgp/crs/misc/ R42511.pdf (last visited Oct. 14, 2015).
[62] *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).
[63] *Id.*

information and history can be preserved online, and can be easily collected by the government in mass quantities.[64] Her lone approach focused on whether the government's ability to collect so much personal information was enabling it to learn about a person's private affairs "more or less at will."[65] More than simply a single concurrence, Sotomayor "penned a legal manifesto on privacy for a digital age debated among Fourth Amendment scholars and brandished by civil libertarians seeking to prevent the coming of a digital government panopticon."[66]

As the *Kyllo* and *Jones* decisions exhibited, the Supreme Court had begun to take on the task as to how the Fourth Amendment applies in the digital world. Those cases also illustrated the difficulties the Court has in determining how developing technology changes Fourth Amendment privacy rights.[67] In the subsequent years, the Court, and the legal community, has continued to attempt to answer questions such as whether Internet users have Fourth Amendment protection. One such attempt has been recently made by Orin Kerr, a legal scholar and professor at George Washington University Law School. Kerr's theories have helped create a general framework that courts can utilize in applying Fourth Amendment safeguards and to determine unreasonable searches and seizures to the Internet.[68]

Kerr's approach addresses "the differences between the facts of physical space and the facts of the Internet" and establishes guidelines for courts to "identify new Fourth Amendment distinctions" in order to apply the amendment to a digital environment."[69] Cases like *Olmstead,*

---

[64] Adam Serwer , *How Sotomayor undermined Obama's NSA*, http://www.msnbc.com/msnbc/how-sotomayor-undermined-obamas-nsa (last visited Oct. 14, 2015).
[65] *Jones*, 132 S. Ct. at 955-956 (Sotomayor, J., concurring).
[66] *Id.*
[67] Shaff, *supra* at 425.
[68] Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005, 1007 (2010).
[69] *Id.*

Katz, *Smith*, and *Jones* all dealt with issues of whether the government's surveillance was done "inside" or "outside" a constitutionally protected area. As the aforementioned cases showed, in the physical world, the inside/outside distinction is paramount for Fourth Amendment search and seizure analysis. Law enforcement, for example, must abide by the inside/outside distinction in the physical world to determine what types of surveillance can be done with, and without, a search warrant.[70] As the Court in *Katz* held, the government does not need any probable cause or warrant to conduct surveillance outside.[71] Hence, so long as a person's conduct is out in the open, it is not protected by the Fourth Amendment. Conversely, in most cases, Fourth Amendment safeguards are triggered when the government enters enclosed spaces like a home[72], an automobile[73], or a sealed package.[74] So, albeit a few clear exceptions, a person presumptively has a reasonable expectation of privacy in "inside spaces."[75]

In the physical world, the line between inside and outside is a crucial element in Fourth Amendment doctrine as it ensures a proper balance between necessary government investigations and personal privacy.[76] In regards to the digital environment, however, there arguably is no "outside." Rather, everything about the Internet seems to be on the "inside" where it is packed into wires and storage devices.[77] As a result, Kerr contends that when facts of criminal investigations switch to the Internet, the physical world "inside/outside distinction no

---

[70] *Id.* at 1009.
[71] "Conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable." *Katz,* 389 U.S. at 361 (Harlan, J., concurring).
[72] "The Fourth Amendment, and the personal rights which it secures, have a long history. At the very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion." *Silverman v. United States*, 365 U.S. 505, 511 (1961).
[73] "Fourth Amendment provides protection to the owner of every container that conceals its contents from plain view," *United States v. Ross*, 456 U.S. 798, 822 (1982).
[74] "Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy and warrantless searches of such effects are presumptively unreasonable." *United States v. Jacobsen, 466 U.S. 109, 114 (1984)*.
[75] Kerr, *supra* at 1011.
[76] *Id.*
[77] *Id.* at 1012.

longer works."[78] Therefore, different rules need to apply; and as Kerr explains, the Internet consequently requires a separate distinction to "mirror the traditional physical distinction" established by the Supreme Court.[79]

Additionally, in the physical world, there is a limit on the scale and location of evidence.[80] Physical evidence normally is limited to a specific location and, accordingly, Fourth Amendment law takes into account those limits.[81] These evidence limits make sense in a physical world and over the years the Court has shaped the Fourth Amendment to coincide with them. In the digital world, however, a very different dynamic exists.[82] Unlike physical evidence, Internet data has no limitations on where it can exist or where it can be stored. For example, a typical Internet user might have multiple e-mail accounts, several social media accounts, and several remote online storage accounts.[83] The Fourth Amendment rules, therefore, that make sense for evidence in the physical world cannot adequately govern Internet evidence. New adapted rules are needed. Kerr suggests new rules in his approach to apply the Fourth Amendment to the Internet.

---

[78] *Id.*
[79] *Id.* at 1009.
[80] *Id.* at 1013.
[81] See *Chimel v. California*, 395 U.S. 752, 763 (1969) ("It is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction. And the area into which an arrestee might reach in order to grab a weapon or evidentiary items must, of course, be governed by a like rule."); See *Arizona v. Gant*, 556 U.S. 332, 351 (2009) ("Police may search a vehicle incident to a recent occupant's arrest only if the arrestee is within reaching distance of the passenger compartment at the time of the search or it is reasonable to believe the vehicle contains evidence of the offense of arrest."); See *United States v. Dunn*, 480 U.S. 294, 294-95 (1987) ("The area claimed to be curtilage is so intimately tied to the home itself that it should be placed under the home's "umbrella" of protection: (1) the proximity of the area to the home; (2) whether the area is within an enclosure surrounding the home; (3) the nature and uses to which the area is put; and (4) the steps taken *295 by the resident to protect the area from observation by passersby."); See *Florida v. Riley*, 488 U.S. 445 (1989) ("the Fourth Amendment does not require the police traveling in the public airways at an altitude of 400 feet to obtain a warrant in order to observe what is visible to the naked eye."); See *Kyllo v. United States*, 533 U.S. 27, 34 (2001) ("obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area constitutes a search—at least where the technology in question is not in general public use.").
[82] Kerr, *supra* at 1014.
[83] *Id.*at 1015.

Attempting to translate and match Fourth Amendment established safeguards from the physical world (i.e. *Katz, Jones)* to the cyber world, Kerr's approach hinges on one main concept. Kerr proposes to replaces the inside/outside distinction of the physical world with a "content/non-content" distinction for the Internet.[84] Referring to *Katz,* Kerr suggests that Internet users should also have a reasonable expectation of privacy in the "contents" of Internet communications but not in "non-content" information.[85] By using narrow comparisons between the physical space and cyberspace, Kerr's privacy application to the Internet articulates the distinction between Internet "content" and "non-content." Specifically, he suggests courts should utilize the physical world privacy language and treat Internet "non-content" information as if it was functionally on the "outside" and Internet "content" information as if it were functionally on the "inside."[86] Under this framework, Internet surveillance of non-content information would not trigger Fourth Amendment protections as physical world surveillance of outside places does not presumptively trigger Fourth Amendment protections. Along these same lines, Internet surveillance of content information would trigger the Fourth Amendment just as physical world surveillance of inside places would presumptively trigger the Fourth Amendment.[87] Therefore, based on Kerr's privacy roadmap, it naturally follow that Internet inside content would be considered a search under the Fourth Amendment. Conversely, Internet non-content would not be considered a search.

According to Kerr, the content/non-content distinction mimics the inside/outside distinction to answer two key questions: 1. What is Internet content? and 2. What is Internet non-content? Just as outside surveillance in the physical world generally relate to identity, location,

[84] *Id.*at 1018.
[85] *Id.*at 1008
[86] *Id.*
[87] *Id.*

and time, Internet non-content would also constitute surveillance related to identity, location, and time.[88] Additionally, just as inside surveillance in the physical world would seek to gather a person's "private thoughts," Internet content surveillance would presumably convey a person's "private thoughts and speech."[89]

With a content/non-content framework in place for the Internet, the courts then would be tasked with drawing the line between the two to determine how the Fourth Amendment applies. Using an analogy for postal mail, Kerr further describes Internet non-content as addressing (or "envelope") information and Internet content as what's inside that "envelope", e.g. the letter itself.[90] Like postal mail, the Internet deals with the sending and delivering of information. Common examples are e-mail and instant messaging. So, under Kerr's content/non-content distinction, the non-content information would be the "to" and "from", while content information would be the actual message itself.[91] According to Kerr, Internet content should include "the substance of our thinking when we assume no else is around."[92] Moreover, it includes the aspects of Internet use intended to be "hidden from those other than the recipients" for a "specific person or even just to ourselves."[93] This vital distinction from non-content allows people to use the Internet for individual purposes or to communicate with others without government intrusion.

The technology of the Internet is evolving at a rapid pace. Despite this clear reality, the courts have yielded only a few decisions dealing with the Fourth Amendment as it applies to

[88] *Id.*
[89] *Id.*
[90] *Id.*at 1019.
[91] Kerr, *supra* at 1019.
[92] *Id.*at 1020.
[93] *Id.*

Internet. Relying on past case law and Professor Kerr's rubric, the next question raised should be: "If Internet content triggers the Fourth Amendment, what exactly is Internet content?"

The Supreme Court attempted to tackle the Internet content/non-content distinction in *City of Ontario v. Quon*.[94] In this 2010 case, the Court set out to determine whether a California police department violated the constitutional rights of an employee when it inspected personal text messages sent and received by a city-owned pager. The case, which required familiarity with the technology behind pagers, produced questions at oral argument which showed a shocking lack of knowledge by the Justices in the area of the Internet.[95]

Perhaps it was a lack of Internet expertise, but the Court in *Quon* never reached the narrow question of the appropriate level of Fourth Amendment protection for Internet content.[96] However, the Court did infer that a person does have a reasonable expectation of privacy in his text messages, even though they could be accessed by a third party (i.e. ISP).[97] But the Court's hesitation in *Quon* to create an Internet content/non-content distinction for Fourth amendment analysis left the Internet privacy question unresolved. In defense of the Court, this is a difficult issue for the Court to resolve as different Internet applications (i.e. email, instant messaging, Uniform Resource Locators (URLs)) are unique in their own way, so the content/non-content distinction therefore must also be unique for each specific mode of communication. With issues unresolved, crucial questions remain open as to whether email subject lines, URLs, website IP addresses should be protected as content or treated as non-content (envelope) information.[98]

---

[94] *City of Ontario v Quon*, 560 U.S. 746 (2010).
[95] "What is the difference between a pager and e-mail?"; "What happens if [an officer] is on the pager and sending a message [when other officers are] trying to reach him ...? Does he get a busy signal?"; "Could [the Plaintiff] print these ... spicy conversations out and circulate them among his buddies?" Transcript of Oral Argument, *Id*.
[96] Land, *supra* at page 8.
[97] *Id.*
[98] Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 Wm. & Mary L. Rev. 2105, 2110-2111 (2009).

As a result of the Court's reluctance to take on the Internet privacy issue, a major content vs. non-content controversy continues regarding the privacy interests of web surfing information (i.e. the IP addresses of websites and the URL addresses of the individual pages viewed.)[99] Supporters of broad privacy protection have expressed concern that URLs contain content and can reveal intimate personal information about web users.[100] Others, conversely, interpret URLs and IP addresses as non-content and rely on the third party doctrine to argue that they are not protected by the Fourth Amendment, no matter what their content status.[101] Most courts addressing the applicability of the Fourth Amendment to the Internet have followed the holding in *Smith* to delineate a clear bright line between content and non-content data[102] Subsequently, courts in the past have held that under third party doctrine, the Fourth Amendment does not apply to email addressing (envelope) information, such as IP and to/from addresses.[103]

For example, the Ninth Circuit tackled the Internet privacy question in 2008.[104] In that case, the court held that the government did not trigger the Fourth Amendment when it had a suspect's Internet service provider install a monitoring device that recorded the IP address, to/from address for emails, and volume sent from the account.[105] Notably, the court did comment on what it considered to be Internet content. The Ninth Circuit tracked the reasoning in *Smith* and held that the Internet surveillance in that case was "indistinguishable" from the use of a pen register device in *Smith.*[106] In regards to Fourth Amendment implications, the court

[99] Tokson, *supra* at 2123.
[100] *Id*.
[101] *Id*.
[102] Molly K.Land, *A Human Rights Perspective on the U.S. Courts and the Constitutional Regulation of the Internet*, http://works.bepress.com/molly_land/16/ (last visited Oct. 16, 2015)
[103] *Id*.
[104] *United States v Forrester,* 512 F.3d 500 (9th Cir. 2008).
[105] Kerr, *supra* at 1027.
[106] *Forrester,* 512 F.3d at 510.

considered IP addresses to be the Internet equivalent of telephone numbers. As a result, under *Smith,* IP addresses were considered non-content and not protected by the Fourth Amendment.[107]

The Sixth Circuit, however, has applied a different Internet content/non-content distinction and has held that Internet e-mail receives Fourth Amendment protection just as telephone calls.[108] The court explained that its holding was based on the current social role of Internet communications.[109] Although the opinion was later vacated on other technical grounds, the Sixth Circuit did ultimately hold that a person "enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial ISP"[110] Therefore, under that rationale, the government cannot rely on the third-party doctrine from *Smith* and "may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable course."[111]

With the Circuit Courts divided, and the Supreme Court seemingly reluctant to solve the internet privacy question, Federal legislation concerning electronic surveillance is similarly inconsistent and lacking. In response to *Katz,* Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III").[112] Because Title III covered only the interception of "wire" and "oral" communications rather than communications generally, the

[107] "When the government obtains the to/from addresses of a person's e-mails or the IP addresses of websites visited, it does not find out the contents of the messages or know the particular pages on the websites the person viewed." *Id.*
[108] "Individuals maintain a reasonable expectation of privacy in e-mails that are stored with, or received through, a commercial ISP." *Warshak v United States,* 490 F.3d 455, 473 (2007).
[109] "Like the telephone earlier in our history, e-mail is an ever-increasing mode of private communication, and protecting shared communications through this medium is as important to Fourth Amendment principles today as protecting telephone conversations has been in the past." *Id.*
[110] *United States v. Warshak,* 631 F.3d 266, 288 (6th Cir. 2010).
[111] *Id.*
[112] Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 Geo. Wash. L. Rev. 1375, 1388 (2004)

development of electronic communications created a gap in the statute. In 1986, Congress sought to fill this gap with the Electronic Communications Privacy Act ("ECPA"). [113]

By supplementing Title III, Congress implemented the ECPA to protect privacy interests in the emerging realm of electronic communications.[114] The ECPA was intended to extend privacy rights to e-mail as well as create new protections for stored communications and stored records held by third parties.[115] At the time, many hailed the legislation as a victory for privacy.[116] But the ECPA was written back in 1986, before most people had computers at home; before laptops, tablets and smartphones changed our lives; before social media and the World Wide Web; and before most people even used email.[117] Within a matter of years, however, the Internet grew and the ECPA became the lone statutory framework for government surveillance of Internet communications. In enacting the ECPA, Congress sought largely to align treatment of electronic communications with Title III's treatment of wire communications. But Congress clearly failed to anticipate that technological developments which ultimately placed so many electronic communications in the hands of third parties.[118]

While the ECPA provides greater protection than the Fourth Amendment in some ways, it provides significant less protection in others.[119] Whereas, under *Smith,* the Court afforded no Fourth Amendment protection for non-content, the ECPA does gives an Internet user some more privacy protection by requiring the government to first obtain a subpoena to obtain non-

---

[113] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).
[114] Mulligan, *supra* at 1557.
[115] *Id*.
[116] Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 Geo. Wash. L. Rev. 1557 (2004).
[117] Grover G. Norquist, Laura Murphy, *A Fourth Amendment Issue Online*, (March 17, 2013 09:40 PM), http://www.politico.com/story/2013/03/grover-norquist-laura-murphy-a-fourth-amendment-application-for-the-internet-088955.
[118] Bellia, *supra* at 1391.
[119] Land, *supra* at 9.

content.[120] However, the ECPA provides less protection than the Fourth Amendment in several other scenarios. Currently, under the ECPA, the government can access the following Internet communications without a warrant: emails older than 6 months, digital address books and calendars, direct Twitter messages older than 6 months, cloud storage documents, Facebook messages and comments older than 6 months, private Facebook and Instagram photos, text message older than 6 months, Dropbox accounts, and search queries.[121] Many in the legal community find the ECPA to be overly outdated because, back in 1986 , email service providers did not store emails for very long after they were sent and read.[122] In 1986, it was practically inconceivable that a service provider would store email for more than 180 days. Therefore, ECPA treated older email almost as if it were abandoned property, allowing a government official to demand it from the service provider with a subpoena issued without a judge's approval.

The degree to which the Internet receives Fourth Amendment provides protection remains an "open question" as "electronic communication via e-mails, text messages, and other means opens a new frontier in Fourth Amendment jurisprudence that has been little explored."[123] With technological development seemingly outpacing judicial review and federal legislation, the question as to whether a person has a reasonable expectation when using the Internet becomes more pressing with each passing day.

[120] *Id.*
[121] *It's Time For A Privacy Update!,* ACLU (last visited Oct. 18, 2015) https://www.aclu.org/infographic/its-time-privacy-update
[122] Norquist, Murphy *supra* note 5.
[123] *Quon v. Arch Wireless Operating Co.,* 529 F.3d 892, 904 (9th Cir. 2008).

Last year, the Supreme Court moved Fourth Amendment doctrine a bit forward with respect to cell phones, which are increasingly the primary way in which people access the Internet. In *Riley v California,*[124] the Court addressed the scope of the search-incident-to-a-lawful arrest exception to the Fourth Amendment's warrant requirement. The Court unanimously held that the search of digital content of cell (smart) phones does not fall within the exception and, absent a warrant, any search would be unconstitutional.[125] The Court reasoned that cell phones "differ in both a quantitative and a qualitative sense" from other physical items that are searchable incident to arrest.[126] Given their "immense storage capacity," Chief Justice Roberts commented in the majority opinion that cellphones "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[127]

The Court's decision in *Riley* represents an important, albeit minor, development for Internet privacy rights. While only in the narrow context of searches incident to arrest, the Court moved the Fourth Amendment further into the digital world by addressing new privacy challenges presented by technological developments.[128] The holding requires a warrant to search any data on a cell phone, regardless of whether that data is saved in the cloud (i.e. in online servers managed by a hosting company), or on the phone's internal hard drive.[129] However, outside of the search incident to an arrest context, the Court did not address whether information stored in the cloud is entitled to Fourth Amendment protection.[130] The Court in fact went out of

[124] *Riley v California,* 134 S.Ct. 2473 (2014).
[125] "The police generally may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested." *Id*. at 2477.
[126] *Id*.
[127] *Id.* at 2489.
[128] Land, *supra* at 9.
[129] Ryan Watzel, *Riley's Implications for Fourth Amendment Protection in the Cloud,* 124 Yale L.J. Forum 73 (2014).
[130] *Id*.

its way to clarify that *Riley* did "not implicate the question of whether the collection or inspection of...digital information amounts to a search under other circumstances."[131] Nonetheless, the decision in *Riley*, while narrow in context, signals a potential shift in the Court's stance on third-party doctrine. Notably, *Riley* acknowledged the Court's concerns with the evolving technological landscape we live in as well as sensitivity towards user content and privacy.

Additional discussion regarding third party doctrine in the digital age took place recently in the DC Circuit. In *Klayman vs Obama,*[132] a federal district court addressed the Government's bulk collection of telephone metadata (i.e. phone numbers dialed, date, and duration). The court distinguished *Smith* and found that third party doctrine did not preclude Fourth Amendment application. In its finding that a national security surveillance program constituted a warrantless search, the DC Circuit concluded that the circumstances in *Klayman* was a "far cry" from the analysis in *Smith.*[133]

Although the telephone data collected in *Klayman* was considered "non-content," the *Klayman* court emphasized the quantity and quality of the information collected in determining that a reasonable expectation of privacy existed.[134] Specifically, the court in *Klayman* found several differences from *Smith* in reaching its conclusion that a Fourth Amendment violation took place. For example, unlike in *Smith* where one specific phone number was monitored, *Klayman* implicated the telephone transactions for millions of U.S. citizens[135] Also, the government's collection of metadata in *Smith* stemmed from an ongoing criminal investigation.

---

[131] *Riley*, 134 S.Ct. at 2489.
[132] *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013) vacated and remanded, 800 F.3d 559 (D.C. Cir. 2015).
[133] *Id.* at 31.
[134] *Id.* at 11.
[135] *Id.* at 33.

In *Klayman*, however, the government, as part of its broad counterterrorism investigation, monitored citizens "without any particularized suspicion of wrongdoing."[136] Additionally, the pen register in *Smith* was utilized for 2 weeks. The surveillance at issue in *Klayman*, however, involved the collection of five years worth of data.[137] In this regard, the court in Klayman added that while metadata has not changed over time, the "ubiquity of phones has dramatically altered the quantity of information that is now available and, more importantly, what that information can tell the Government about people's lives."[138] Here, the court addressed the non-content vs content distinction and held that "people in 2013" had "an entirely different relationship with phone" than those that lived back during the *Smith* case. The *Klayman* court suggested over the course of five years, the content/non-content distinction begins to break down.[139] In other words, if the government can collect enough non-content (e.g. metadata), content can ultimately be derived from it.

While the decision in *Klayman* was recently vacated due to a standing issue, the case has significantly furthered the dialogue of the privacy rights in the digital age. *Klayman* called upon the Supreme Court to reread *Smith* and reconsider third party doctrine by factoring in "present day circumstances," "the evolution of the government's surveillance capabilities," and "citizens' phone habits."[140] To that end, in considering *Klayman*, the Court should conclude that the precedent in *Smith* can no longer apply.[141] Although *Klayman* addressed privacy rights solely in the context of telephone use, perspectives from that case support a vision of the Fourth Amendment being sensitive both to technological change and to context. Based on the rapidly

[136] *Id.* at 30.
[137] *Id.* at 32.
[138] *Id.* at 35-36.
[139] *Id.* at 36.
[140] *Id.* at 31.
[141] *Id*.

expanding change in the digital world, the analysis in *Klayman* should ultimately extend to Internet privacy rights as well.

The Internet privacy right issue has recently fueled an emerging debate over encryption. Specifically, in response to demands from Internet users requesting higher levels of privacy and security, companies like Google and Apple have been rolling out stronger "end-to-end" encryption on their devices and services, such as iPhones and Gmail.[142] End-to-end encryption is a method of digital communication where the only the sender and recipient of a message have access to it. The "end-to-end" promise means that messages are encrypted in such a way that allows only the unique recipient of a message to decrypt it, and not anyone in between, not even the Internet providers, i.e. Google and Apple.[143]

The encryption methods implemented by companies like Google and Apple have arguably created a reasonable expectation of privacy for users of the Internet. Encryption offers a much needed protection for users as their smartphones have become the modern day equivalent of "digital homes."[144] This added privacy protection has gotten the attention of FBI and the Department. Specifically, in the name of criminal and national security investigations, these government agencies have insisted that Google and Apple need to provide them with "back doors" to access private Internet communications.[145]

Providing backdoors to the government, however, as privacy and cryptology experts have maintained, would be impossible without compromising the security of computer systems and opening holes for criminals to exploit. Nonetheless, the FBI and DOJ continue to put pressure

---

[142] Jenna McLaughlin, *FBI and DOJ Target New Enemy In Crypto Wars: Apple and Google*, (July 8, 2015 2:10 PM), https://theintercept.com/2015/07/08/fbi-doj-name-new-enemy-crypto-wars-apple-google/
[143] Andy Greenberg, *Hacker Lexicon: What is End-to-End Encryption?*, (Nov. 25, 2014 9:00 AM), http://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/
[144] Wayne Rash, *FBI Director Ignores 4th Amendment in Call for Encryption 'Back Doors',* (Oct. 16, 2014), http://www.eweek.com/print/security/fbi-director-ignores-4th-amendment-in-call-for-encryption-back-doors.html
[145] McLaughlin, *supra* note 3.

on companies like Apple and Google to comply with their requests. The agencies contend that end-to-end encryption poses an "every day" problem and an "insurmountable barrier" in conducting surveillance. Yet according to a Federal Courts report on wiretapping in 2014, state and federal law enforcement encountered only four cases all year (out of 3,554) in which wiretaps were ineffective because of encryption.[146] While it's fair to acknowledge that, due to encryption, the FBI and DOJ may have a diminished capacity to conduct some investigations, it's also fair to recognize that, at some point, an appropriate balance between safety, privacy, and liberty must be struck.

As this paper is being written, Internet privacy rights are far from secure. The challenges posed by the intersection of the Fourth Amendment, Federal legislation, and Internet surveillance are not easy ones. The constitutional and statutory frameworks governing electronic surveillance law developed at a time when electronic communications either did not exist or were not widely used.[147] The Internet and other technological developments have subsequently placed tremendous strain on those frameworks.[148] The essential elements of ECPA have not changed since 1986, and the Supreme Court has failed to keep pace, saying remarkably little about the Fourth Amendment's application to new technology.[149] Hence, the government can contend the ECPA gives it the authority to ignore Internet privacy to an extent that would have "shocked the framers of the Constitution."[150]

While there is still significant work to be done, some progress has been made. Building on the decisions in *Katz, Smith, and Kyllo*, recent cases like *Jones* and *Riley* have produced some

[146] *Wiretap Report 2014 / United States Courts,* (last updated on Dec. 31, 2014), http://www.uscourts.gov/statistics-reports/wiretap-report-2014.
[147] *Bellia, supra* at 1458.
[148] *Bellia, supra* at 1458.
[149] Norquist, Murphy *supra* note 7.
[150] *Id.*

clarification in the balance between electronic surveillance and privacy. Despite their differing ideologies, Justices Scalia and Sotomayor have furthered the discussion in their own way to frame the rules of searches and third-party doctrine; and to further clarify standards for "reasonableness" and "expectation of privacy." Similarly, scholars like Orin Kerr have contributed by offering theories to adapt and modernize legal doctrine into the world of the Internet and new technologies. Moreover, companies like Apple and Google have entered into the Internet privacy fray by instituting encryption protection for their customers. In the end, time will tell as to whether the Supreme Court and Congress can strike a fair and appropriate balance between Internet privacy rights and transparency.